February 2, 2005

Acquisition

Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems (D-2005-033)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **02 FEB 2005**	2. REPORT TYPE **N/A**	3. DATES COVERED -

4. TITLE AND SUBTITLE **Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**34**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

February 2, 2005

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/CHIEF INFORMATION OFFICER
NAVAL INSPECTOR GENERAL

SUBJECT: Report on Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems (Report No. D-2005-033)

We are providing this report for review and comment. We considered management comments from the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space on a draft of this report when preparing the final report. This report is the third in a series of reports that discusses the implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Navy.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not provide comments; therefore, Recommendations A.1. and A.2. remain unresolved. We request that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer provide comments on this final report that conform to the requirements of DoD Directive 7650.3 by March 2, 2005. No further comments are required from the Navy.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Audam@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Mr. Robert L. Shaffer at (703) 604-9043 (DSN 664-9043). See Appendix C for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Mary L. Ugone
Assistant Inspector General
for Acquisition and Technology Management

Office of the Inspector General of the Department of Defense

Report No. D-2005-033 **February 2, 2005**
(Project No. D2004AL-0011)

Implementation of the Interoperability and Information Assurance Policies for Acquisition of Navy Systems

Executive Summary

Who Should Read This Report and Why? Civilian and military managers who are responsible for interoperability and information assurance requirements of Navy systems should read this report because it addresses the importance of adhering to DoD interoperability and information assurance policies to reduce the risk of Navy systems not being interoperable and being unable to exchange information in a secure manner with other DoD and allied systems.

Background. This report is the third in a series of reports on the implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Navy. The first report addressed the implementation of those policies within the Office of the Secretary of Defense and the Defense agencies. The second report addressed how effectively the Army implemented those policies. The fourth report will address how effectively the Air Force implemented those policies.

Results. The Navy had not implemented DoD policy to populate and maintain the inventory of Global Information Grid assets. As a result, all applicable Navy sensors, weapon systems, and business systems will not be included in the DoD enterprise-wide inventory of Global Information Grid assets, and DoD will not be able obtain the information superiority necessary for the Services to accomplish their assigned missions effectively and efficiently. The Assistant Secretary of Defense for Networks and Information Integration needs to prepare and staff a DoD Directive that specifies the types of systems and system information capabilities to be included in the inventory of Global Information Grid assets and the responsibilities of the DoD Components to populate and maintain it (finding A).

The Navy had not fully implemented interoperability policies to prepare or update required acquisition documents. Without documents that address interoperability, capability, and supportability, DoD cannot be assured that its systems will be compatible with existing systems, will meet the information needs of U.S. forces, or be interoperable with proposed systems. The Chief of Naval Operations in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy Command, Control, Communications, Computers, Intelligence and Space should require system program managers to obtain Joint Staff J-6 certification for a system’s interoperability requirements, to prepare and use information support plans for all systems throughout the life of the system, and to prepare system security authorization agreements for systems that are subject to the DoD Information Technology Security Certification and Accreditation Process (finding B). See the Findings section of the report for the detailed recommendations.

Management Comments and Audit Response. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not comment on the December 17, 2004, draft report. Therefore, we request that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer provide comments on this final report by March 2, 2005. The Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space concurred with the findings and recommendations. See the Findings section of the report for a discussion of the management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Findings

Appendixes

Management Comments

Background

This report is the third in a series of reports on DoD implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the Navy's implementation of those policies on the inventory for Global Information Grid assets and the provision of the required documentation.

Chairman of the Joint Chiefs of Staff Testimony on the President's Proposed Defense Program for Fiscal Year 2005. On February 4, 2004, General Pace, the Vice Chairman of the Joint Chiefs of Staff, testified before the U.S. House of Representatives Committee on Armed Services. General Pace described how information sharing is critical for planning and executing military operations. He testified that:

> Since this is a global war requiring an international effort, we must also improve coalition command and control capabilities, and consolidate the numerous networks that exist today. These disparate networks hinder our ability to plan in a collaborative environment and exercise timely and effective command and control with our multinational partners.
>
> We must also review policies and implementing technology that safeguard our vital sensitive information while ensuring critical operational information is shared with all those who fight beside us. JFCOM [Joint Forces Command] has been tasked to take the lead in identifying specific multinational information sharing requirements and recommending policy changes. Our goal is to establish a multinational family of systems with common standards as part of the Global Information Grid enterprise services. I view this as a top priority and ask for Congressional support- information sharing with our allies is critical to winning the War on Terrorism.

Top Ten Priorities. The Secretary of Defense issued a list of the top ten DoD priorities for August 2003 through December 2004. One of those priorities is to strengthen joint warfighting capabilities to develop joint concepts to integrate air, land, and sea operations, and to strengthen joint exercises and joint training. Strengthening joint warfighting capabilities will enhance interoperability and communication among warfighters.

Joint Operations Concepts. In November 2003, the Secretary of Defense issued the Joint Operations Concepts, which describes the overarching concept for conducting future joint military operations. The Joint Operations Concepts provided the operational concept for transforming the Armed Forces to achieve joint force capabilities. The Joint Operations Concepts states that the joint force will leverage technology to provide actionable, precise, and "fused" intelligence at all levels of war to facilitate decision superiority. To facilitate decision superiority, the joint force must gain and maintain information superiority. Achieving these capabilities will require a singular battlespace networked to enable continuous and collaborative campaign planning and an adaptive command and control organization. Upon achieving decision superiority, the joint force can defeat any adversary or control any situation across the full range of military operations when the joint force is integrated and networked and interoperable with interagency and multinational partners.

Scope of Navy Programs Surveyed. We judgmentally selected and reviewed 40 Navy programs from the Office of the Secretary of Defense Test and Evaluation Oversight List for 2003. We sent a questionnaire to each program office to survey their awareness of interoperability and information assurance requirements and to determine whether their system was part of the inventory for Global Information Grid assets. Appendix B lists the Navy programs surveyed. We also requested program offices to provide the following documents:

- operational requirements document;
- command, control, communications, computers, and intelligence support plan;
- test and evaluation master plan; and
- system security authorization agreement.

Overall Audit Project. This project is a continuation of work reported in Inspector General of the Department of Defense Report No. D-2003-011, "Implementation of Interoperability and Information Assurance Polices for Acquisition of DoD Weapon Systems," October 17, 2002, which addressed whether the Office of the Secretary of Defense and DoD agencies were effectively implementing DoD interoperability and information assurance policies. Report No. D-2004-008, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems," October 15, 2003, addressed the adequacy of interoperability and information assurance requirements for Army systems. Concurrent with this audit, another review is assessing how effectively the Air Force is implementing DoD interoperability and information assurance policies.

Objectives

The primary audit objective was to evaluate whether the Navy was effectively implementing DoD interoperability and information assurance policies. Specifically, the audit determined whether the Navy was effectively identifying system interoperability and information assurance requirements in the requirements generation process. See Appendix A for a discussion of the audit scope and methodology and prior coverage related to the audit objectives.

A. Implementing Global Information Grid Policies

The Navy had not implemented DoD policy to populate and maintain the inventory for Global Information Grid assets because DoD guidance is not clear on the types of systems and system information capability requirements that should be included. As a result, all applicable Navy sensors, weapon systems, and business systems will not be included in the DoD enterprise-wide inventory of Global Information Grid assets, and DoD will not be able obtain the information superiority necessary for the Services to accomplish their assigned missions effectively and efficiently.

Guidance

Federal Information Security Management Act of 2002. On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347) that included Title III, "Federal Information Security Management Act of 2002." Section 305 of the Act, "Technical and Conforming Amendments," requires DoD to develop and maintain an inventory of major information systems, including major national security systems, operated under its control. Section 301, Subchapter III, section 3542, "Definitions," states that national security systems include information systems used or operated by an agency or contracted by an agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or is critical to direct fulfillment of military or intelligence missions.

Public Law 105-261. Section 2223, title 10, United States Code, chapter 131, "Information Technology: Additional Responsibilities of Chief Information Officers," October 17, 1998, requires the DoD Chief Information Officer to maintain a consolidated inventory of DoD mission-critical and mission-essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

DoD Directive 4630.5. DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004, updates DoD policy and responsibilities for interoperability and supportability of system information technology, including national security systems. The Directive requires the DoD Chief Information Officer to ensure the development, implementation, and maintenance of the Global Information Grid architecture in accordance with DoD Directive 8100.1.

DoD Directive 8100.1. DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002, establishes policy and assigns responsibilities for the configuration management and architecture of the Global Information Grid. The Directive states that it is DoD policy that an enterprise-wide inventory of Global Information Grid assets shall be established and maintained. Further, the Directive requires the:

- Under Secretary of Defense for Acquisition, Technology, and Logistics to ensure that acquisition programs fully consider documented Global Information Grid requirements and architecture;

- Under Secretary of Defense (Comptroller) to collaborate with the DoD Chief Information Officer, where necessary, to identify and coordinate improvements to the identification and portrayal of information technology resources to improve overall information technology visibility;

- DoD Components, including the Joint Chiefs of Staff and the Under Secretary of Defense for Acquisition, Technology, and Logistics, to populate and maintain their portions of the inventory for Global Information Grid assets; and

- Chairman of the Joint Chiefs of Staff to develop joint doctrine and ensure that Chairman of the Joint Chiefs of Staff Instructions are compatible with Global Information Grid policy and guidance.

DoD Directive 8100.1 further states that the Global Information Grid includes any system, equipment, software, or service that meets one or more of the following criteria:

- transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services;

- provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, or services; or

- processes data or information for use by other equipment, software, or services.

Inventory for Navy Global Information Grid Assets

The Navy had not implemented DoD policy to populate and maintain the inventory for Global Information Grid assets.

Program Office Awareness of the Global Information Grid Policy. We surveyed Navy program offices responsible for 40 systems and asked the program officials whether they considered their systems to be part of the inventory for Global Information Grid assets. Navy program office responses for 40 systems were that:

- 19 of the systems were part of the inventory,
- 18 of the systems were not part of the inventory, and
- 3 Navy program offices were not sure whether their systems were part of the inventory.

Systems, Equipment, Software, and Services not Designated as Global Information Grid Assets. In response to our survey, Navy program offices provided the following reasons why 11 of the18 systems were not reported as part of the inventory for Global Information Grid assets.

- 1 system predated the Global Information Grid overarching policy,
- 9 systems communicated only with the host platform or were part of another system, and
- 1 system was a weapon system.

Navy program offices did not explain why seven other systems--the F/A-18E/F Super Hornet Naval Strike Fighter, CVN-68 Nimitz Class Nuclear-Powered Aircraft Carrier, LPD-17 San Antonio Class Amphibious Transport Dock Ship, T-AKE Auxiliary Cargo and Ammunition Ship, Tactical Control System, KC-130J Hercules Tactical Aerial Refueler, and Integrated Electronic Defensive Countermeasures--were not considered part of the inventory for Global Information Grid assets. For example, the operational requirements document for the F/A-18E/F includes interoperability as a performance parameter and program officials stated that it will be certified for interoperability by the Joint Interoperability Test Command; however, the program office did not consider the F/A-18E/F to be a Global Information Grid asset.

Navy program offices were not sure whether three additional systems--the E-2C Reproduction Hawkeye Airborne Early Warning Aircraft, the EX 171 Extended Range Guided Munition, and the T-45TS Training Aircraft--should be part of the inventory for Global Information Grid assets. For example, program officials for the EX 171 Extended Range Guided Munition program office stated that they thought their program should be part of the inventory for Global Information Grid assets but did not know what action to take.

The E-2C Reproduction Hawkeye Airborne Early Warning Aircraft and the RIM-162 Evolved Sea Sparrow Missile are national security systems and should be Global Information Grid assets. The program office considered the AN/BQQ-10 Acoustic Rapid Commercial-Off-The-Shelf Insertion, which is a system included on a submarine, to be a Global Information Grid asset based on the criteria in DoD Directive 8100.1. However, program officials did not consider the AN/ALR-67(V)3 Advanced Special Receiver and the AN/SPY-1D(V) Radar as Global Information Grid assets because they are part of another system. Because a system communicates only with its host platform or is part of another system may not be sufficient justification to exclude the system from the inventory for Global Information Grid assets.

Need to Clearly Define Global Information Grid Asset Inventory Guidance. The Navy had not implemented DoD policy on the Global Information Grid because DoD guidance is not clear on the types of systems and system information that should be included in the inventory. The criteria in DoD Directive 8100.1, outlining which system, equipment, software, or service should be included in the Global Information Grid, is so broad that virtually all Navy systems should be included. Navy systems may meet one of the criteria for inclusion in the Global Information Grid asset inventory, but they do not necessarily contribute to a network-based way of fighting to achieve information superiority, enable joint mission planning, and execute more timely military operations and battlefield assessments. In addition, each Navy program office may interpret the criteria differently in choosing which systems to include in the inventory for Global Information Grid assets.

Effect on Populating and Maintaining the Global Information Grid Asset Inventory

Without a clearly defined policy on the types of systems and system information capability requirements that should be included in the inventory for Global Information Grid assets and how the inventory will be maintained, Navy program offices may be incorrectly designating systems as Global Information Grid or non-Global Information Grid assets. Therefore, DoD will not realize its goal of including most sensors, weapon systems, and business systems into the Global Information Grid to obtain information superiority for the Services to accomplish their assigned missions.

Conclusion

Specific guidance needs to be issued on the types of systems and information capability requirements that are necessary for a globally interconnected, end-to-end, interoperable, and secure system-of-systems to meet the DoD joint warfighting needs. With the necessary guidance, DoD will be able to concentrate its resources on those systems that will meet its vision of collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Recommendation and Management Comments

A. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer prepare and staff a DoD Directive that specifies the:

1. Types of systems and system information capability requirements to be included in the inventory for Global Information Grid assets.

2. Responsibilities of DoD Components in populating and maintaining the inventory for Global Information Grid assets.

Management Comments Required. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not provide comments on the December 17, 2004, draft report. Therefore, we request the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer provide comments on the final report by March 2, 2005.

Navy Comments. The Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space concurred that the Department of the Navy has not implemented DoD policy to populate and maintain the inventory for the Global Information Grid because DoD guidance was not clear on the types of systems and system information capability requirements that should be included. The Deputy Assistant Secretary stated that the Department of the Navy Chief Information Officer has maintained a database of mission essential and mission critical information technology systems, including those in platforms and weapons systems. In addition, the Deputy Assistant Secretary stated that the Chief Information Officer is involved in the creation of the DoD Information Technology Program Repository that will catalog systems and applications across the DoD and serve as the information technology systems registry for DoD.

B. Implementing Interoperability Policies

The Navy did not fully implement interoperability policies to prepare or update required acquisition documents because responsible Navy officials did not ensure that system program offices identified interoperability requirements and included those requirements in acquisition documents throughout the life of the system. Without documents that address interoperability, capability, and supportability, DoD cannot provide assurance that systems being developed, acquired, and deployed meet the information needs of U.S. forces, are interoperable with existing and proposed systems, and are supported by the Global Information Grid.

Guidance

DoD Policy. DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004, establishes the net-ready key performance parameter, which replaced the interoperability key performance parameter and incorporated net-centric concepts for achieving information technology and national security system interoperability and supportability. The Directive requires DoD Components to ensure that interoperability and supportability capabilities are designed, developed, incorporated, tested, and evaluated for all their information technology and national security systems. In addition, the Directive requires DoD Components to develop procedures for the acquisition of all information technology and national security systems and to document, manage, evaluate, and report on interoperability, supportability, and sufficiency throughout a system's life using an information support plan.

DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004, states that DoD Components must develop an information support plan , which was formerly known as the command, control, communication, computers, and intelligence support plan, for all acquisition programs to document the program's interoperability, information, and support requirements and that it be maintained throughout the acquisition life cycle. The Joint Interoperability Test Command evaluates and certifies all acquisition information technology and national security systems for interoperability. This report uses the term "command, control, communication, computers, and intelligence support plan" because programs reviewed during the audit usually provided command, control, communication, computers, and intelligence support plans.

The Instruction requires the heads of the DoD Components to:

- require the Chief Information Officer to ensure that the Component complies with DoD Instruction 4630.8;

- ensure that information support plans for all acquisition-category and nonacquisition-category acquisitions are prepared;

- identify and document in an information support plan a net-ready key performance parameter for all acquisition-category, nonacquisition-category, and fielded information technology and national security system acquisitions;

- submit the information support plan to the cognizant authority for review and validation; and

- ensure interoperability, supportability, and information assurance are designed, developed, tested, evaluated, and incorporated into all DoD Component information technology and national security systems.

DoD Instruction 5000.2, “Operation of the Defense Acquisition System,” May 12, 2003, states that, during system development and demonstration, the capabilities development document, which was formerly known as the operational requirements document, will state the detailed operational performance parameters. Further, the Instruction states that the capabilities production document will state the operational requirements resulting from system development and demonstration and will detail the performance expected of the production system; however, this report uses the term “operational requirements document” because programs reviewed during the audit usually provided operational requirements documents.

DoD Instruction 5200.40, “Defense Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, applies to all DoD Components and shall be used in the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. The Instruction applies to the life cycle of any information technology or information system, the development of new systems, and the upgrade of existing and legacy systems. Further, the Instruction states that the key to the Defense Information Technology Security Certification and Accreditation Process is the agreement between the information technology system program manager, the designated approving authority, the certification authority, and the user representative to resolve critical schedule, budget, security, and performance issues. This agreement is documented in the system security authorization agreement and is used to guide the certification and accreditation process. The system security authorization agreement establishes a binding agreement on the level of security required before system development or changes may begin.

Joint Staff Policy. Chairman of the Joint Chiefs of Staff Instruction 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," November 20, 2003, establishes policies and procedures for the process to achieve Joint Staff J-6 interoperability and supportability certification. The Joint Staff Instruction also provides additional guidance for developing information support plans and establishes procedures for certification of requirements in the information support plans. The Joint Staff J-6 must recertify interoperability when material changes such as hardware, firmware, or software modifications affect interoperability, and every 3 years when the certifications expire. Establishing system interoperability and supportability is a continuous process that must be managed throughout the life cycle of the system. This Joint Staff Instruction applies to all information technology and national security systems that DoD acquires, procures, or operates. In addition, the Joint Staff Instruction states that all information technology and national security systems will be compliant with the Clinger-Cohen Act, DoD interoperability regulations and policies, and the guidance for the DoD Information Technology Standards Registry.

Navy Policy. Secretary of the Navy Instruction 5000.2B, "Implementation of Mandatory Procedures for Major and Non-Major Defense Acquisition Programs and Major and Non-Major Information Technology Acquisition Programs," December 6, 1996, states that the Chief of Naval Operations and the Commandant of the Marine Corps are responsible for ensuring that the required documentation is provided. In addition, the Navy Instruction states that operational requirements documents must include clearly defined, joint interoperability requirements, or state that joint interoperability is not required. All operational requirements documents with a command, control, communications, computers and intelligence element will be staffed for a review of impact and interoperability. The Navy Instruction further states that operational requirements documents related to command, control, communications, computers and intelligence will be forwarded to the Joint Staff J-6 for interoperability certification.

Chief of Naval Operations Instruction 5239.1B, "Navy Information Assurance (IA) Program," November 9, 1999, states that the Chief of Naval Operations is responsible for directing implementation of the Navy information assurance program in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space (formerly the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence/Electronic Warfare/Space) in compliance with DoD Instruction 5200.40.

Navy Information Assurance Publication 5239-13, "Information Assurance Certification and Accreditation," December 2000, provides guidance for implementing Chief of Naval Operations Instruction 5239.1B.

Acquisition Documents

The Navy did not fully implement interoperability policies to prepare or update required acquisition documents, such as operational requirements documents; command, control, communications, computers, and intelligence support plans; and system security authorization agreements. In addition, the Navy did not obtain Joint Staff J-6 certification of interoperability requirements. We requested those acquisition documents from Navy program offices for the 40 systems that we selected and reviewed.

Operational Requirements Documents. The Navy program offices provided the operational requirements documents for 26 of the 40 systems that we selected and reviewed. We reviewed those documents to determine whether the interoperability requirements were key performance parameters that could be measured, tested, and evaluated. Thirteen of the 26 operational requirements documents contained a net-ready, key performance parameter. Navy program offices stated that interoperability was not a key performance parameter in the remaining 13 operational requirements documents. Reasons given were that:

- 2 systems had operational requirements documents that were being updated to include interoperability as a key performance parameter,
- 2 systems communicated only with the host platform,
- 4 systems are part of other systems, and
- 5 systems predated the requirement for interoperability certification and have not had any subsequent milestone decisions.

Operational Requirements Documents not Provided. Navy program offices did not provide operational requirements documents for 14 of the systems that we selected and reviewed. The Navy gave the following reasons for not providing an operational requirements document:

- 6 systems predated the requirement for interoperability certification and have not had any subsequent milestone decisions,
- 3 systems had operational requirements documents that were being updated to include interoperability as a key performance parameter,
- 1 system was not considered an acquisition program,
- 2 systems did not have an interoperability requirement, and

The program offices for the remaining two systems stated that their operational requirements documents were certified for interoperability by the Joint Staff J-6; however, the program offices did not provide those documents for our review.

Need to Update Requirements Documentation. Although the Nimitz Nuclear Powered Aircraft Carrier (CVN) and both the LHD-1 and

LHD-8 Amphibious Assault Ship programs did not require DoD 5000 series documentation at their inception, both classes of ships are still being built. In addition, the LHD-8 was changed from an Acquisition Category II to an Acquisition Category 1C program. At that time, the operational requirements documents should have been prepared to address interoperability as a key performance parameter.

Joint Staff J-6 Certifications. Navy program offices responded to the survey for the 40 systems that we selected and reviewed and stated that the operational requirements documents for 10 systems were certified for interoperability by the Joint Staff J-6. In addition, Joint Staff J-6 interoperability certification was planned or in process for 10 other systems, including 4 that did not have an operational requirements document as part of their program documentation. Of the 20 systems that were not certified for interoperability by the Joint Staff J-6:

- 4 systems did not require an operational requirements document at program inception;

- 8 systems were initiated before the interoperability certification became a requirement;

- 6 systems did not have an interoperability requirement, communicated only with the host platform, or were part of another system; and

- 2 program offices were unsure whether the operational requirements documents for their systems had been certified for interoperability by the Joint Staff J-6.

Need to Obtain Interoperability Certifications. Examples of Global Information Grid assets that were initiated before the Joint Staff J-6 was required to certify interoperability were the SSN-21 Seawolf Submarine, the DDG-51 Guided Missile Destroyer, and the LHD-1 and LHD-8 Amphibious Assault Ships. Examples of systems that were not Global Information Grid assets, but should have been, that were initiated before Joint Staff J-6 was required to certify interoperability were the CVN-68 Aircraft Carrier and the E-2C Early Warning Command and Control aircraft. The Joint Interoperability Test Command certified the Seawolf Submarine’s AN/BSY-2 Combat Control System as meeting some of its interoperability requirements; however, the Command did not certify the overall system because the operational requirements document lacked interoperability key performance parameters and information exchange requirements. In addition, although the LHD-8 Amphibious Assault Ship, which is currently under construction, does not have an operational requirements document, the program office stated that the Joint Interoperability Test Command will certify the system for interoperability. Interoperability certifications should be obtained to ensure that the systems are interoperable with existing and planned systems of joint, combined, and coalition forces.

Command, Control, Communications, Computers, and Intelligence Support Plans. Navy program offices provided command, control, communications, computers, and intelligence support plans for only 17 of the 40 Navy systems that we selected and reviewed. DoD Instruction 4630.8 states that DoD Components must develop a command, control, communication, computers, and intelligence support plan for all acquisition programs to document the program's interoperability, information, and support requirements and that the plan be maintained throughout the acquisition life cycle. We did not determine the adequacy of the support plans. Navy program offices provided the following explanations for why they did not provide command, control, communications, computer and intelligence support plans.

- 5 systems' command, control, communications, computers, and intelligence support plan were either planned or being prepared.

- 6 systems were initiated before there was a requirement to prepare a command, control, communications, computers, and intelligence support plan;

- 10 systems communicated only with the host platform, were part of another system, or interoperability requirements did not apply; and

- 1 system was a Commercial-Off-The-Shelf program without milestones or key performance parameters.

The program office for the remaining system did not give a reason why a command, control, communications, computers and intelligence support plan was not provided.

Although program offices stated that support plans were not prepared because the requirement did not exist at the time the systems were initiated, systems communicated only with their host platform, or were part of other systems, other program offices with similar systems prepared the required documentation. A command, control, communications, computer and intelligence support plan was being prepared for the E-2C Reproduction Hawkeye Airborne Early Warning Aircraft, although the requirement was not in effect when the program was initiated. In addition, support plans were prepared for the Remote Airborne Mine Clearance System and the RIM-162 Evolved Sea Sparrow Missile, although they communicate only with the host platform, and the Integrated Defensive Electronic Countermeasure System, which is part of another system.

System Security Authorization Agreements. During our review of 40 Navy systems surveyed, we determined that Navy program managers were not always preparing system security authorization agreements for all systems with information technology requirements. DoD Instruction 5200.40 states that the key to the Defense Information Technology Security Certification and Accreditation Process is the agreement between the information technology system program manager, the designated approving authority, the certification authority, and the user representative to resolve critical schedule, budget, security, and performance issues. This agreement is documented in the system security authorization agreement and is used to guide the certification and accreditation process. The system security authorization agreement establishes a binding agreement on the level of security required before system development or changes may begin. The Instruction applies to the life cycle of any information technology or information system, the development of new systems, and the upgrade of existing and legacy systems.

Preparation of System Security Authorization Agreements. Navy program offices provided system security authorization agreements for only 11 of the 40 systems that we selected and reviewed. We did not determine whether the contents of the system security authorization agreements were adequate. Reasons given for not providing system security authorization agreements were:

- 11 systems' security authorization agreements were planned or being prepared;
- 12 systems communicate only with the host platform, were part of another system, or interoperability requirements did not apply;
- 4 systems were initiated before preparation of a system security authorization agreement became a requirement; and
- 1 system had a program security instruction instead of a system security authorization agreement.

The program office for the remaining system did not give a reason why a system security authorization agreement was not provided.

The Federal Information Security Management Act, Office of Management and Budget reporting instructions, and the DoD Information Technical Security Certification and Accreditation Process contain requirements for security and security plans. In addition, although program offices provided several reasons for not preparing system security authorization agreements, other program offices with similar system requirements had prepared system security authorization agreements. For example, a system security authorization agreement was prepared for the SSN-21 Seawolf Class Nuclear-Powered Attack Submarine and the Ship Self Defense System, even though the requirement was not in effect when the programs were initiated. In addition, a system security authorization agreement was being prepared for the AN/BQQ-10 Acoustic Rapid Commercial-Off-The-Shelf Insertion, although it is part of another system and communicates only with the host platform.

Effect of Not Implementing Interoperability Policies

A system should not be excluded from meeting interoperability requirements because the program was initiated before interoperability certification was required. The Chief of Naval Operations and the Assistant Secretary of the Navy (Research, Development and Acquisition) are responsible for ensuring that interoperability requirements of systems are included in the acquisition documents. According to the capstone requirements document for the Global

Information Grid, the success of the Global Information Grid depends on how well it helps achieve interoperability to allow force-wide sharing of information; however, the capstone requirements document states that some information systems that are already fielded may not support the timely flow of accurate and relevant information needed to meet future joint warfighting needs. In addition, legacy systems are not normally designed to support global end-to end network management or adhere to a prescribed set of interoperability standards for the DoD and intelligence communities. Interoperability requirements should be established for systems that communicate with other systems and certified by the Joint Staff J-6 to better support the DoD vision of a joint force that will attain information superiority and meet future joint warfighting needs. Without management oversight and strict implementation of requirements for acquisition documents, the Navy has no assurance that fielded systems are compatible with existing command, control, communications, computer and intelligence infrastructure of other DoD systems. The systems may not be adequate to meet the information needs; interface requirements; and net-centric, interoperability, and supportability concerns that will enable forces to operate effectively in joint, combined, coalition, and interagency operations.

Recommendations and Management Comments

The Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space concurred with the findings and recommendations. Specific comments on each recommendation follow.

B.1. We recommend that the Chief of Naval Operations in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space require system program managers to:

a. Obtain Joint Staff J-6 certification for systems with interoperability requirements that support joint warfighting needs, including systems that were initiated before the interoperability certification became a requirement, systems that are still being built, systems that have undergone major modifications, and systems that are included in the inventory of Global Information Grid assets.

Navy Comments. The Deputy Assistant Secretary stated that the Department of the Navy is planning to achieve substantial compliance with "FORCEnet" technical standards by September 2010, when major portions of the DoD net-centric architecture are expected to be in place for net-centric operations.

b. Prepare and use information support plans for all systems with information technology requirements to document interoperability and supportability requirements, or provide written justification stating why an information support plan is not required.

Navy Comments. The Deputy Assistant Secretary concurred that written justification should be required for any program that does not prepare an Information Support Plan.

c. Prepare system security authorization agreements for systems that are subject to the DoD Information Technology Security Certification and Accreditation Process.

Navy Comments. The Deputy Assistant Secretary stated that a better definition of when or what security is required in accordance with DoD Instruction 5100.40 was needed to provide common compliance across the Navy. The Deputy Assistant Secretary also stated that the Chief Information Officer, Department of the Navy and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space review and assess information assurance strategies for all major programs prior to milestone approval or award of contracts acquiring information technology systems.

B.2. We recommend that the Chief of Naval Operations in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence and Space establish specific accountability processes to verify that system program managers accomplish the actions specified in Recommendation B.1.

Navy Comments. The Deputy Assistant Secretary stated that accountability practices are being conducted but some refinement, clarification, and discipline in the Navy processes may be necessary to ensure that program managers execute their responsibilities for joint staff certification, information support plans and system security authorization agreements. The Deputy Assistant Secretary further stated that the Navy will continue efforts like the “FORCEnet” Implementation Baseline and Policy to support existing processes to ensure program managers execute their responsibilities for joint staff certification, information support plans and system security authorization agreements when appropriate and notify programs when they are not.

Appendix A. Scope and Methodology

We reviewed documentation dated from December 1965 to June 2004. To accomplish the audit objective, we reviewed:

- the Navy's efforts to implement interoperability and information assurance requirements during the acquisition process,
- requirements documentation for interoperability and information assurance requirements, and
- applicable criteria.

We also contacted the staff of the Chief Information Officer, Department of the Navy.

In addition, we judgmentally selected and reviewed 40 Navy systems from the Office of the Secretary of Defense Test and Evaluation Oversight List. A questionnaire was used to obtain program managers' perspectives on interoperability and information assurance requirements. We also requested operational requirements documents; command, control, communications, computers, and intelligence support plans; and system security authorization agreements for each system.

We performed this audit from November 2003 through December 2004 in accordance with generally accepted government auditing standards. We did not review the management control program because the audit focused on the interoperability and information assurance requirements and review processes; therefore, our scope was limited to those specific requirements and processes.

Government Accountability Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the DoD weapon system acquisition high-risk area.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the Government Accountability Office and the Inspector General of the Department of Defense have issued seven reports addressing interoperability and information assurance requirements for DoD systems. Unrestricted Government Accountability Office and Inspector General of the Department of Defense reports can be accessed at http://www.gao.gov and http://www.dodig.osd.mil/audit/reports, respectively.

Government Accountability Office (GAO)

GAO Report No. GAO-04-858, “Defense Acquisitions – The Global Information Grid and Challenges Facing its Implementation,” July 2004

GAO Report No. GAO-03-329, “Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data,” March 2003

Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2004-008, “Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems,” October 15, 2003

IG DoD Report No. D-2003-024, “Information Assurance Challenges – An Evaluation of Audit Results Reported From August 23, 2001, through July 31, 2002,” November 21, 2002

IG DoD Report No. D-2003-011, “Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems,” October 17, 2002

IG DoD Report No. D-2001-176, “Survey of Acquisition Manager Experience using the DoD Joint Technical Architecture in the Acquisition Process,” August 22, 2001

IG DoD Report No. D-2001-121, “Use of the DoD Joint Technical Architecture in the Acquisition Process,” May 14, 2001

Appendix B. Navy Programs Reviewed

1. E-2C Reproduction Hawkeye Airborne Early Warning Aircraft
2. F/A 18 E/F Super Hornet Naval Strike Fighter
3. KC-130J Hercules Tactical Aerial Refueler
4. MH-60R Seahawk Multi-Mission Helicopter Upgrade
5. Multi-Mission Maritime Aircraft
6. V-22 Osprey Joint Advanced Vertical Lift Aircraft
7. CVN 68 Nimitz Class Nuclear-Powered Aircraft Carriers
8. LHD-8 Amphibious Assault Ship
9. LHA (R) Amphibious Assault Ship
10. LPD-17 Amphibious Assault Ship
11. SSN-21 Seawolf Class Nuclear-Powered Attack Submarine
12. SSN-774 Virginia Class Nuclear-Powered Attack Submarine
13. DDG-51 Guided Missile Destroyer
14. DD (X) Destroyer
15. T-AKE Lewis and Clark Class of Auxiliary Dry Cargo Ships
16. AGM-84H/K Standoff Land Attack Missile – Expanded Response
17. AARGM/AGM – 88E Advanced Anti-Radiation Guided Missile
18. AIM-9X Air-to-Air Missile Upgrade
19. MK 48 Torpedo Mods
20. Airborne Mine Neutralization System
21. EX-171 Extended Range Guided Missile
22. Rapid Airborne Mine Clearance System
23. RIM-162 Evolved Sea Sparrow Missile
24. Standard Missile-2
25. RIM-116A Rolling Airframe Missile
26. AN/ALR-67(V)3 Advanced Special Receiver
27. BQQ-10 Acoustic Rapid Commercial-Off-The-Shelf Insertion
28. AN/SPY-1 B/D Aegis Multi-Function Phased-Array Radar
29. Joint Mission Planning System
30. Ship Self Defense System
31. Tactical Control System
32. Expeditionary Fighting Vehicle
33. Defense Integrated Military Human Resource System
34. Deployable Joint Command and Control
35. Integrated Defensive Electronic Countermeasure
36. Joint Standoff Weapon Baseline/BLU-108/Unitar
37. Navy Standard Integrated Personnel System
38. Navy-Marine Corps Intranet
39. T-45TS Undergraduate Jet Pilot Training System
40. LHD-1 Amphibious Assault Ship

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense for Networks and Information Integration/Chief
    Information Officer
Director, Operational Test and Evaluation
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff
    Director for Command, Control, Communication and Computer Systems
        Directorate (J-6)

Department of the Navy

Assistant Secretary of the Navy (Research, Development and Acquisition)
    Deputy Assistant Secretary of the Navy for Command, Control, Communications,
        Computers, Intelligence and Space
Chief of Naval Operations
Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

Director, Defense Information System Agency
    Commander, Joint Interoperability Test Command

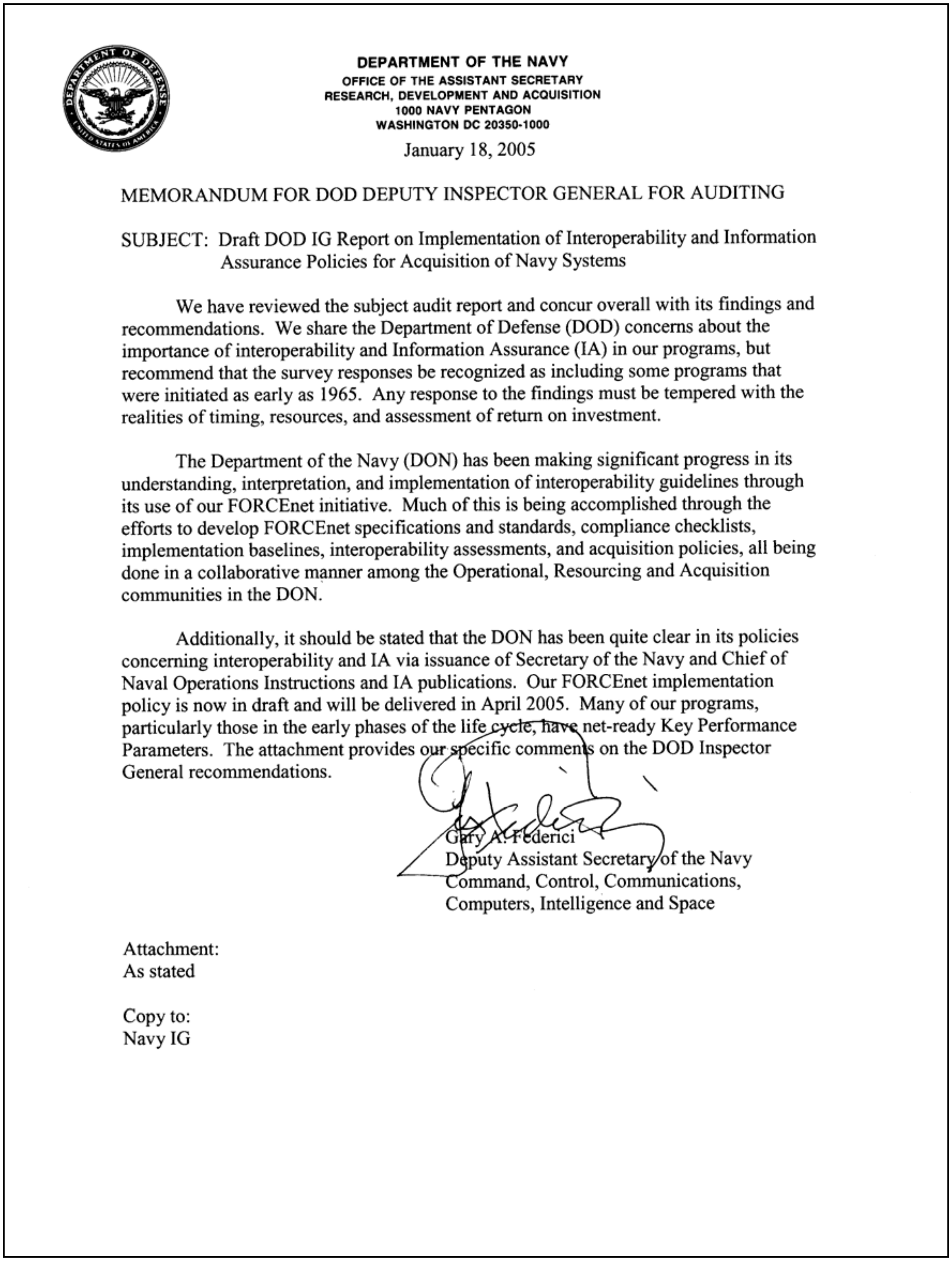
Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Department of the Navy Comments



DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

January 18, 2005

MEMORANDUM FOR DOD DEPUTY INSPECTOR GENERAL FOR AUDITING

SUBJECT: Draft DOD IG Report on Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems

We have reviewed the subject audit report and concur overall with its findings and recommendations. We share the Department of Defense (DOD) concerns about the importance of interoperability and Information Assurance (IA) in our programs, but recommend that the survey responses be recognized as including some programs that were initiated as early as 1965. Any response to the findings must be tempered with the realities of timing, resources, and assessment of return on investment.

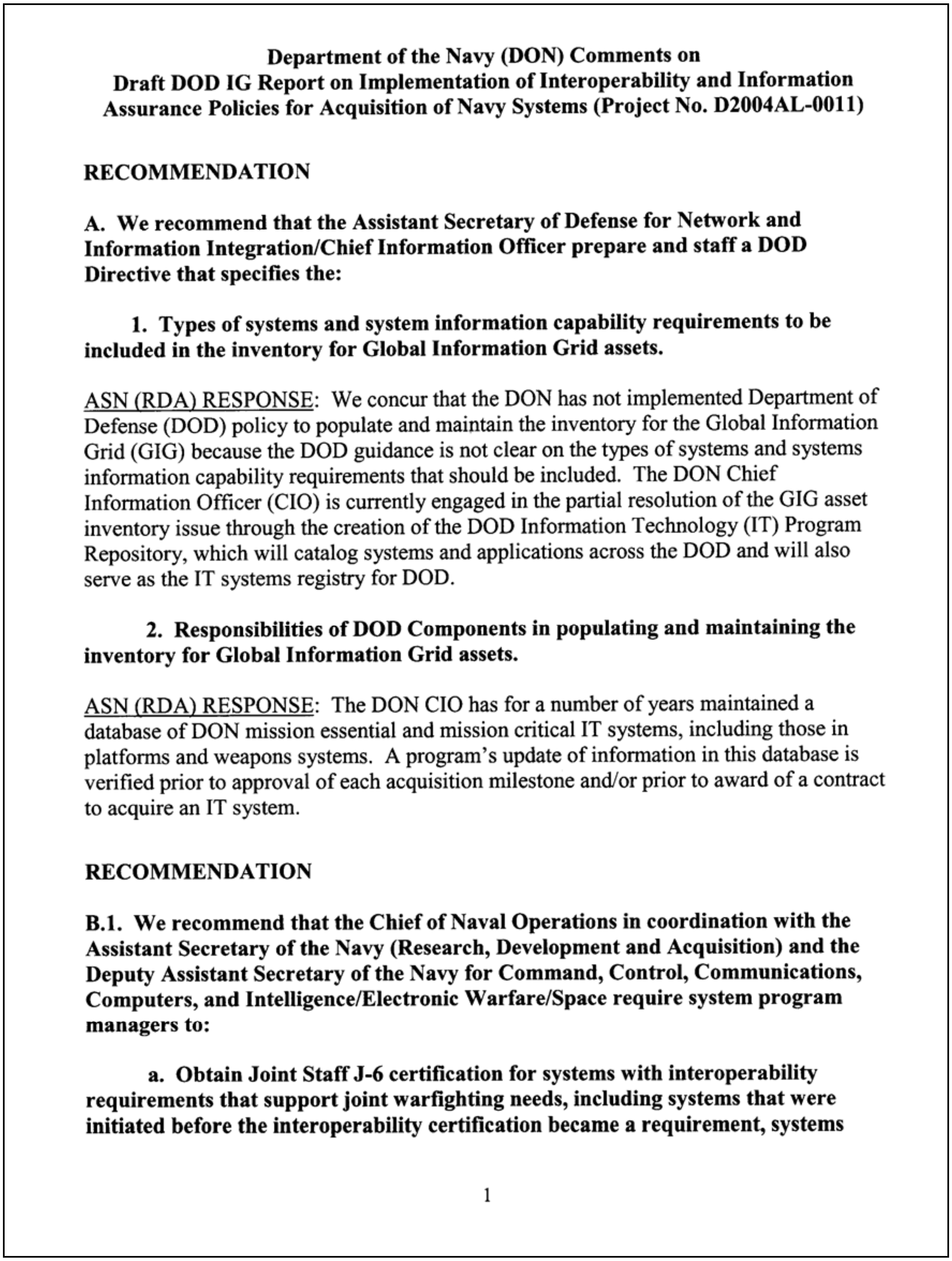
The Department of the Navy (DON) has been making significant progress in its understanding, interpretation, and implementation of interoperability guidelines through its use of our FORCEnet initiative. Much of this is being accomplished through the efforts to develop FORCEnet specifications and standards, compliance checklists, implementation baselines, interoperability assessments, and acquisition policies, all being done in a collaborative manner among the Operational, Resourcing and Acquisition communities in the DON.

Additionally, it should be stated that the DON has been quite clear in its policies concerning interoperability and IA via issuance of Secretary of the Navy and Chief of Naval Operations Instructions and IA publications. Our FORCEnet implementation policy is now in draft and will be delivered in April 2005. Many of our programs, particularly those in the early phases of the life cycle, have net-ready Key Performance Parameters. The attachment provides our specific comments on the DOD Inspector General recommendations.

Gary A. Federici
Deputy Assistant Secretary of the Navy
Command, Control, Communications,
Computers, Intelligence and Space

Attachment:
As stated

Copy to:
Navy IG



Department of the Navy (DON) Comments on
Draft DOD IG Report on Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems (Project No. D2004AL-0011)

RECOMMENDATION

A. We recommend that the Assistant Secretary of Defense for Network and Information Integration/Chief Information Officer prepare and staff a DOD Directive that specifies the:

1. Types of systems and system information capability requirements to be included in the inventory for Global Information Grid assets.

ASN (RDA) RESPONSE: We concur that the DON has not implemented Department of Defense (DOD) policy to populate and maintain the inventory for the Global Information Grid (GIG) because the DOD guidance is not clear on the types of systems and systems information capability requirements that should be included. The DON Chief Information Officer (CIO) is currently engaged in the partial resolution of the GIG asset inventory issue through the creation of the DOD Information Technology (IT) Program Repository, which will catalog systems and applications across the DOD and will also serve as the IT systems registry for DOD.

2. Responsibilities of DOD Components in populating and maintaining the inventory for Global Information Grid assets.

ASN (RDA) RESPONSE: The DON CIO has for a number of years maintained a database of DON mission essential and mission critical IT systems, including those in platforms and weapons systems. A program's update of information in this database is verified prior to approval of each acquisition milestone and/or prior to award of a contract to acquire an IT system.

RECOMMENDATION

B.1. We recommend that the Chief of Naval Operations in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, and Intelligence/Electronic Warfare/Space require system program managers to:

a. Obtain Joint Staff J-6 certification for systems with interoperability requirements that support joint warfighting needs, including systems that were initiated before the interoperability certification became a requirement, systems

that are still being built, systems that have undergone major modifications, and systems that are included in the inventory of Global Information Grid assets.

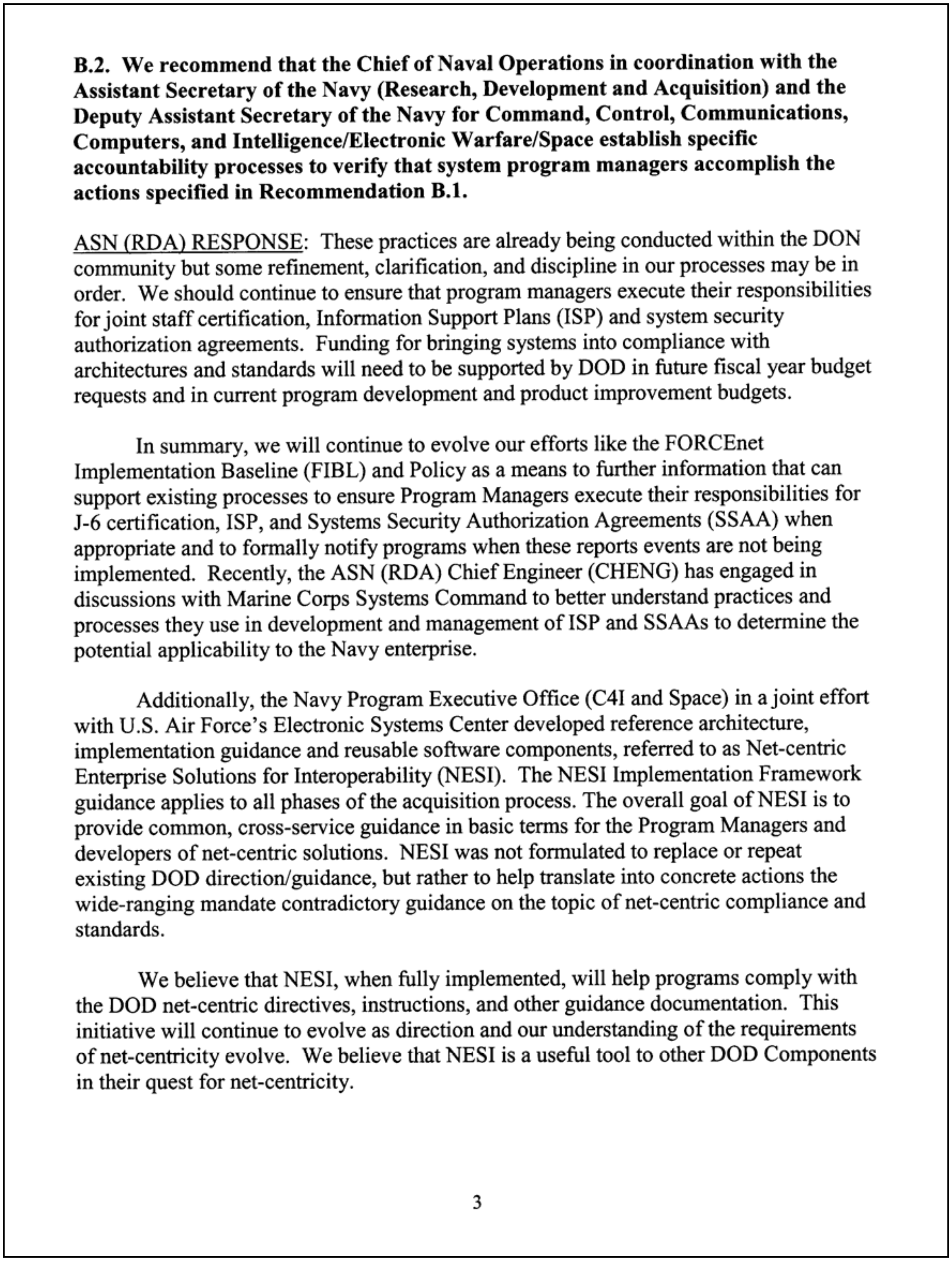
ASN (RDA) RESPONSE: The DON has been quite clear in its policies concerning interoperability and IA via issuance of Secretary of the Navy and Chief of Naval Operations Instructions and IA publications. Many of our programs, particularly those in the early phases of the life cycle, have net-ready Key Performance Parameters (KPPs). We would advise caution in requiring interoperability KPPs for all programs regardless of the program's mission and its current place in the life cycle phase. Resources should be allocated to those programs where the return on investment is the greatest. Program Managers should advise acquisition officials of the cost of achieving compliance along with associated impact on delivery schedule/quantity or performance risk. In its implementation of FORCEnet programs, the DON is planning to achieve substantial compliance with FORCEnet technical standards by September 2010. This is the period during which major portions of the DoD net-centric architecture are expected to be in place to enable net-centric operations. DON acquisitions will accomplish FORCEnet compliance through budget requests, ensuring that appropriate FORCEnet standards are used in program development, and demonstration of FORCEnet compliance at milestone reviews and during developmental and operational testing.

b. Prepare and use information support plans for all systems with information technology requirements to document interoperability and supportability requirements, or provide written justification stating why an information support plan is not required.

ASN (RDA) RESPONSE: We concur that written justification should be required for any program that does not prepare an Information Support Plan. In the DON, test and evaluation for acquisition programs assesses the system's compliance with applicable technical standards and its ability to function in the applicable Families of Systems/Services as defined in the Information Support Plan (ISP).

c. Prepare system security authorization agreements for systems that are subject to the DOD Information Technology Security Certification and Accreditation Process.

ASN (RDA) RESPONSE: Better definition of when/what security is required in accordance with DOD Instruction 51000.40 is needed to provide common compliance across the DON. The DON CIO and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence and Space (DASN (C4I/S)) review and assess IA Strategies for all major programs prior to milestone approval and/or prior to award of contracts acquiring IT systems.



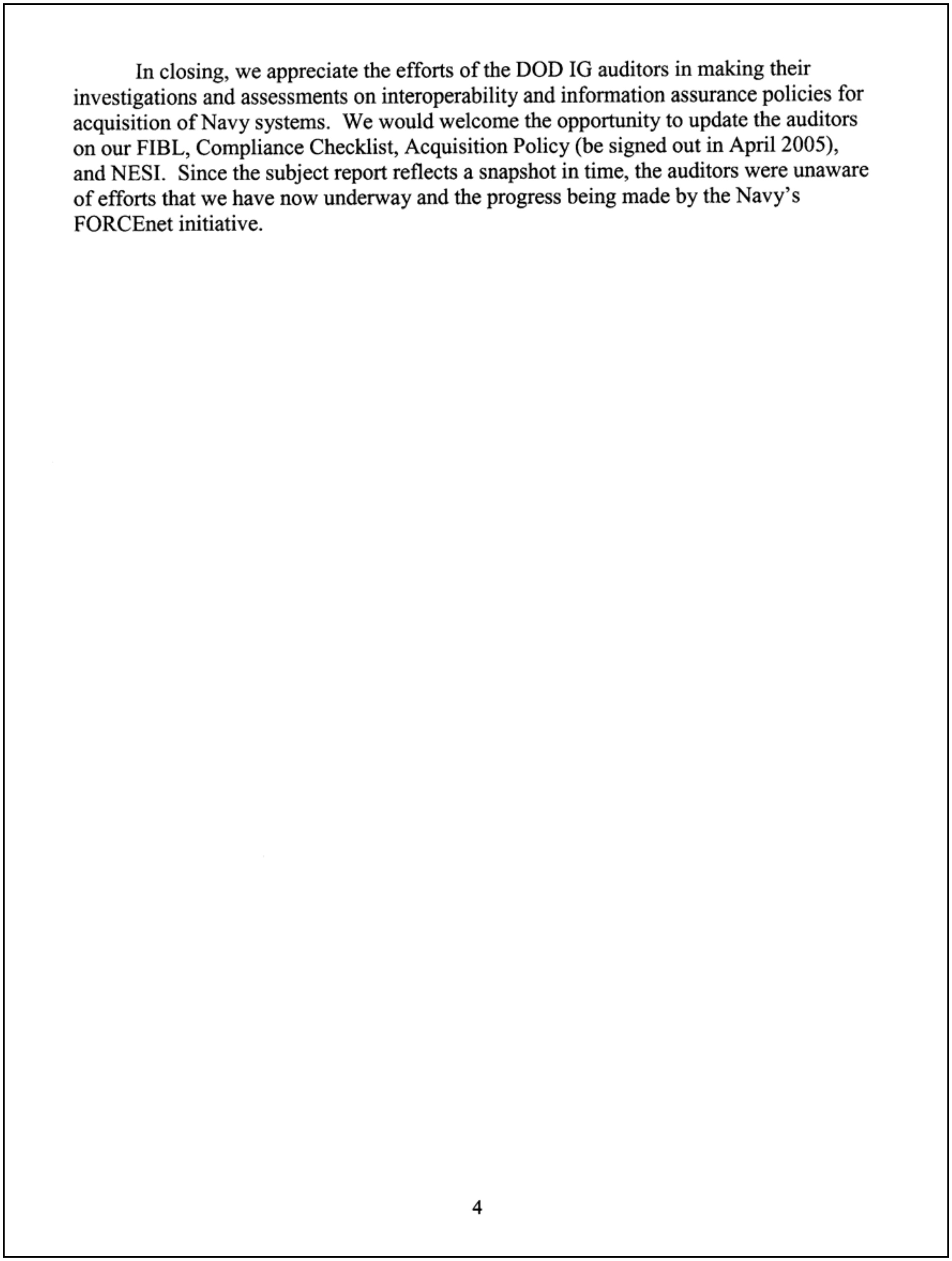
B.2. We recommend that the Chief of Naval Operations in coordination with the Assistant Secretary of the Navy (Research, Development and Acquisition) and the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, and Intelligence/Electronic Warfare/Space establish specific accountability processes to verify that system program managers accomplish the actions specified in Recommendation B.1.

ASN (RDA) RESPONSE: These practices are already being conducted within the DON community but some refinement, clarification, and discipline in our processes may be in order. We should continue to ensure that program managers execute their responsibilities for joint staff certification, Information Support Plans (ISP) and system security authorization agreements. Funding for bringing systems into compliance with architectures and standards will need to be supported by DOD in future fiscal year budget requests and in current program development and product improvement budgets.

In summary, we will continue to evolve our efforts like the FORCEnet Implementation Baseline (FIBL) and Policy as a means to further information that can support existing processes to ensure Program Managers execute their responsibilities for J-6 certification, ISP, and Systems Security Authorization Agreements (SSAA) when appropriate and to formally notify programs when these reports events are not being implemented. Recently, the ASN (RDA) Chief Engineer (CHENG) has engaged in discussions with Marine Corps Systems Command to better understand practices and processes they use in development and management of ISP and SSAAs to determine the potential applicability to the Navy enterprise.

Additionally, the Navy Program Executive Office (C4I and Space) in a joint effort with U.S. Air Force's Electronic Systems Center developed reference architecture, implementation guidance and reusable software components, referred to as Net-centric Enterprise Solutions for Interoperability (NESI). The NESI Implementation Framework guidance applies to all phases of the acquisition process. The overall goal of NESI is to provide common, cross-service guidance in basic terms for the Program Managers and developers of net-centric solutions. NESI was not formulated to replace or repeat existing DOD direction/guidance, but rather to help translate into concrete actions the wide-ranging mandate contradictory guidance on the topic of net-centric compliance and standards.

We believe that NESI, when fully implemented, will help programs comply with the DOD net-centric directives, instructions, and other guidance documentation. This initiative will continue to evolve as direction and our understanding of the requirements of net-centricity evolve. We believe that NESI is a useful tool to other DOD Components in their quest for net-centricity.



In closing, we appreciate the efforts of the DOD IG auditors in making their investigations and assessments on interoperability and information assurance policies for acquisition of Navy systems. We would welcome the opportunity to update the auditors on our FIBL, Compliance Checklist, Acquisition Policy (be signed out in April 2005), and NESI. Since the subject report reflects a snapshot in time, the auditors were unaware of efforts that we have now underway and the progress being made by the Navy's FORCEnet initiative.

Team Members

The Office of the Deputy Inspector General for Auditing of the Department of Defense, Acquisition and Technology Management prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Yolanda D. Bailey
James A. Hoyt
Patricia A. Joyner
Nephateria N. Moore
Jacqueline N. Pugh
Christopher M. Scrabis
Robert L. Shaffer
Kathryn M. Truex
Zachary M. Williams